Fraud awareness

There has been a recent resurgence of incidents across the VPS where scammers have used fraudulent documents to change an existing supplier's bank account details and divert payments to illegitimate bank accounts.

What you can do about it

Agency management are responsible for systems of internal control designed to prevent and detect fraud.

To improve the chances of identifying suspicious requests, you can strengthen preventative controls before the suppliers' bank account changes are processed and updated in the supplier master file database.

We recommend greater vigilance is applied to requests to change supplier bank account details by:

- Treating all supplier bank account change requests with suspicion until you can prove they are legitimate.
- Creating a checklist detailing the processes for staff to follow when performing a change to supplier bank account details and signing off to confirm that all steps have been performed.
- Developing validation techniques such as a phone call to the supplier, or payment protection software solutions that are independent to the supplier requesting the change, to confirm the validity of the change request.
- Asking the supplier to confirm what their old bank account details are and check the details match against the agencies' current records.
- Updating policies and procedures for bank account changes to reflect these additional control activities, and communicate changes to staff.
- Providing additional training to staff to promote fraud awareness, in particular for staff who are more vulnerable to scammers given their role and responsibility.

July 2021

VAGO
Victorian Auditor-General's Office